Efficient way in sharing of IoT data and uses of blockchain in auditing the stored data

Ackley Joseph Lyimo* and Kakelli Anil Kumar

School of Computer Science and Engineering,
Vellore Institute of Technology,
Vellore-632014, Tamil Nadu, India
Email: ackleymilita92@gmail.com
Email: anilsekumar@gmail.com
*Corresponding author

Abstract: Today the need for technology in various aspects of life has risen abruptly, hence leading to the expansion of the internet of things (IoT), but when it comes to IoT data, there is a myriad of issues regarding controlling and auditing it. A lack of measures taken for security can also make IoT vulnerable to a number of threats. To better maintain and minimise these threats, using blockchain can play a significant role by auditing and recording all actions that occur while collecting the data and storing the same in the cloud. Due to the nature of consensus methods in a blockchain system, we introduced the uses of the interplanetary file system wherein the data collected will be stored in them and a hash value will be retrieved which will be sent to the blockchain and recorded. In this paper, we introduced better blockchain-based design for IoT which can show the distributed control of how IoT data is collected, recorded for auditing and stored. Through this system we succeeded in achieving secure sharing of IoT data and proper utilisation of cloud storage resources.

Keywords: blockchain; internet of things; IoT; interplanetary file systems; IPFS.

Reference to this paper should be made as follows: Lyimo, A.J. and Kumar, K.A. (2022) 'Efficient way in sharing of IoT data and uses of blockchain in auditing the stored data', *Int. J. Internet Technology and Secured Transactions*, Vol. 12, No. 1, pp.38–48.

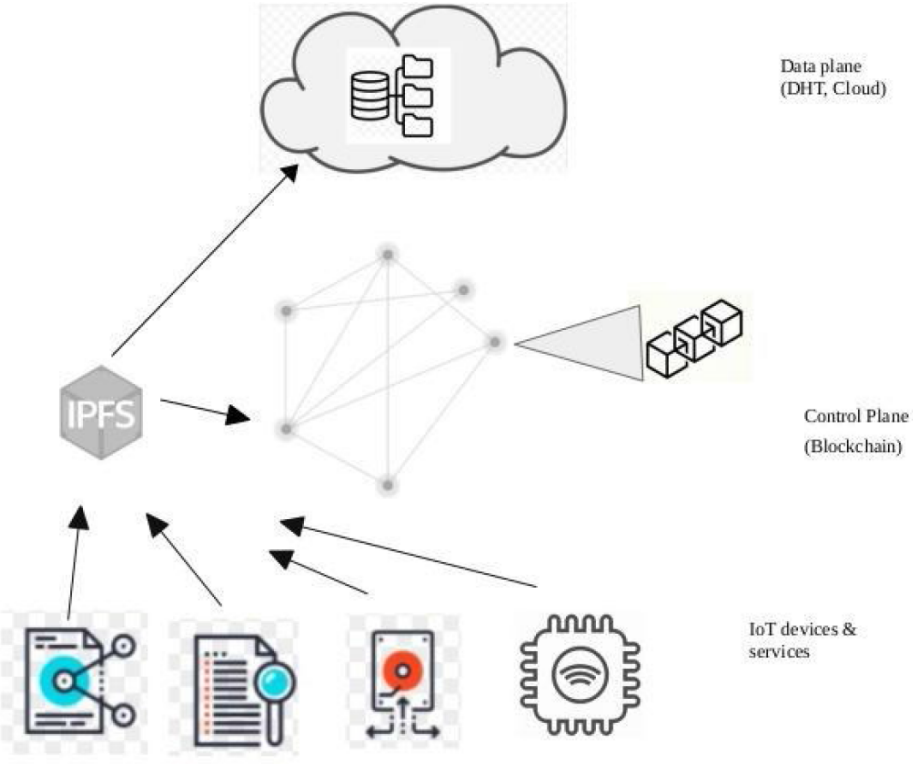
Biographical notes: Ackley Joseph Lyimo received his BTech in Electronic, and Communication Engineering from Jawaharlal Nehru Technological University Anantapur of India in 2016. He is currently doing his MTech in Computer Science and Engineering specialised in information security at Vellore Institute of Technology, Vellore in India.

Kakelli Anil Kumar is an Associate Professor of School of Computer Science and Engineering in Vellore Institute of Technology (VIT), Vellore, TN, India. He earned his PhD in Computer Science and Engineering from Jawaharlal Nehru Technological University (JNTUH) Hyderabad in 2017, and graduated in 2009 and finished his undergraduate studies in 2003 from the same university. He started his teaching career in 2004 and worked as an Assistant Professor, and Associate Professor and HOD in various reputed engineering institutions of India. His current research includes the wireless sensor networks, internet of things (IoT), digital forensics, cyber security, malware analysis, blockchain and crypto-currency. He has published over 35 research articles in reputed peer reviewed international journals and conferences.

1 Introduction

In today's world, most of the time we are surrounded by sensors that measure, detect and send data in various ways. The devices and technologies connected over the internet of things (IoT) can observe, analyse or estimate data in real-time, and this data can offer important understanding to help spare time, energy and resources. But how is IoT data handled and investigated? We are observing an ever-increasing number of ground breaking technologies with the advent of networked embedded devices called the IoT. The current IoT ecosystem typically consists of dedicated low-power devices fitted with data-gathering sensors. This data is then stored in third-party cloud storage through special-purpose apps (i.e., application-layer gateways) for further processing. The data management is based on blockchain and end-to-end encryption with decentralisation. There is no trusted central authority controls the access to user data as shown in Figure 1.

Figure 1 Data management based on blockchain, end-to-end encryption, and decentralisation (see online version for colours)



Note: No trusted central authority controls for the access to user data

As we observed in Zachariah et al. (2015), the design architecture led to isolated data. So, the users have restricted control over their data. Hence, the users have to rely on and trust the cloud provider over their data and since they have no choice so have to count on the promise given to them over the availability and security of their data. In terms of security in IoT the aspect in minimised the vulnerable of the system extremely less as possible

especially in point to point communication and also performs the auditing especially to the required access. For the current and still existed cloud-based model in IoT can still handle Identification, Authentication and also connectivity. However, they still face in terms of the integrity of data. And enhance the third party to be existences (Zhang et al., 2015).

For the better performance the idea of blockchain can be the good proposed for IoT (Panarello et al., 2018) in security design. The technology behind the blockchain is capable of being immutable, auditable, transparency (depend when is permissionless blockchain such as public blockchain), data encryption and so on. Although the blockchain consensus mechanisms tend to be varied for different block chain in term of creating a block. For instance, the estimated block time in bitcoin is 10 minutes (Wright, 2019), while in Ethereum it's between 10 and 19 seconds. In order to maintain hence some technique has to be more done.

The concept of this paper will show how to secure and store the IoT data in cloud and auditing the blockchain can exhibit successful in

1 cryptographically secure data sharing and storage utilisation

2 use of Ethereum blockchain and smart contract in successfully stored hash from IPFS in order to further auditing (Shafagh et al., 2017; Zhang and Lee, 2020a).

The remainder of this paper is structured according to the following Section 2 we discuss the related works, Section 3 we provide an overview layout of the system proposed and explain the structure of the system followed by tests and analyse in Section 4, and finally Section 5 will be conclusions.

2 Literature survey

From the system we briefly reviewed some relative work done in previous system. Lodderstedt et al. (2013) introduce notion of data sharing in the web services on the OAuth protocol. They consider trusted central Author authority to enforce the user define access policies. However, it did not satisfy the decentralised and auditable access control in management.

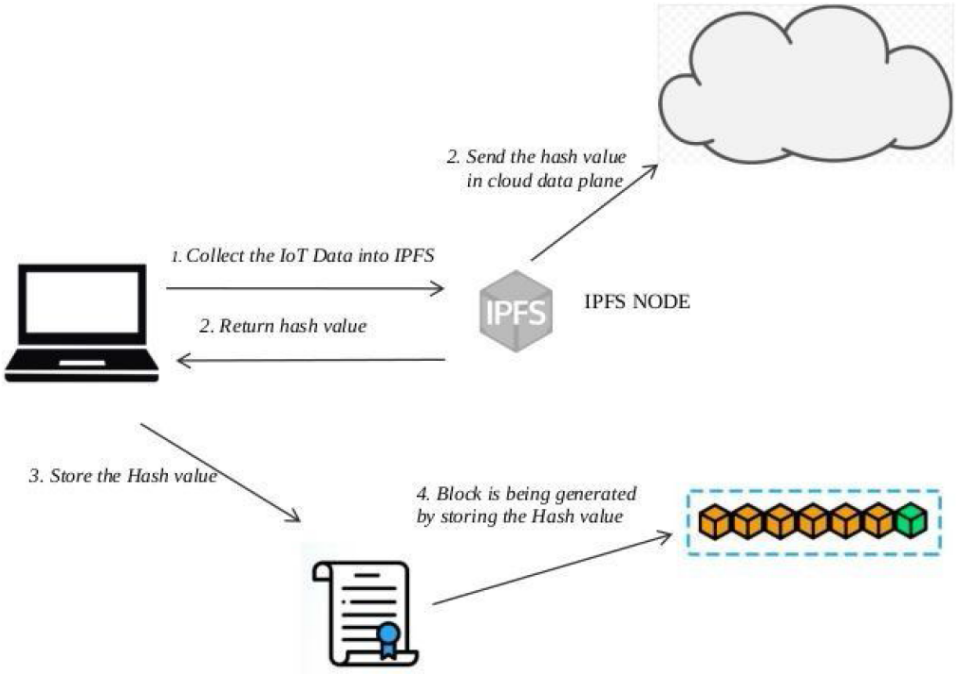
Xie et al. (2017) addresses the issue in secure data storage based on the collecting agriculture product data. They introduce a double-chain storage based on blockchain. Due to the issue of tracking it might be able to be open to most of the users in the decentralised network (during using blockchain). However, they issue of utilising of double-chain storage was not satisfying at all.

Ali et al. (2016) came up with the concept of virtual chains and suggest a server-less decentralised DNS. The concept is known as block-stack and extends to decentralised public key distribution system and user integrity registry. Similarly, Filecoin (Benet and Greco, 2018) and Storj (Wilkinson et al., 2014) have addressed the issue of distributed storage of the object. Both are intended for file *Efficient way In Sharing of IoT data and uses of Blockchain in Auditing the storage data* archiving but lack sharing function.

3 Proposed system

From our design we force actually in two-layer includes control plane and data plane, hence according to our distributed storage system we decoupled them. The control plane will used in auditing and distributing the access control layer to the storage while the data plane would consider as storage plane. The reason of using this is order to satisfy decentralised, resilient and auditable access control management as shown in Figure 2.

Figure 2 Proposed blockchain system with IPFS (see online version for colours)



In an aspect of the control plane we consider blockchain as a control in auditing. In term of our proposed we employed the use of Ethereum as our present candidate for the blockchain layer as our reference of security. Since it provides an immutable data storage where existing transactions cannot be updated or deleted. Cryptography and digital signatures are used to prove identity and authenticity. The nature of the consensus time consumes by Ethereum in generating the blocks is 19 to 20 sec. Hence, we introduced the uses of IPFS it can collect the data file/image at certainty. And stored them and retrieve hash value generated and stored it in blockchain with the guidance of smart contracts (Tikhomirov et al., 2018). In the data plane we used in order to satisfy the secure data storage. So, consider as conventional data plane Cloud provider stores the hash data submitted by the Interplanetary File system in the file-sharing scenario using easy cloud storage. In this case, how the cloud provider can manage those files isn't clear to the users. The quality and availability of files often do not come with its services (Ion et al., 2011). Even the credibility of files is included in their service level agreement (SLA), users of files cannot check it unless they put extra effort into doing so. We can only trust the cloud provider for provenance that can be unfavourable (Asghar et al., 2012).

3.1 Control plane

In the control plane we consider two-aspect whereby we introduced the two techniques to be considered.

- *Interplanetary file storage (IPFS):* This is peer to peer decentralised network protocol that involves distributing of files by connecting computing devices in the same system of files. IPFS provides a high data throughput since is based on the content-based addressing (Carzaniga et al., 2000). Hence does not required central server. The IPFS allows any node that has a connection to the network can able to retrieve and store data for them by 'pinning' content actively. The major use of IPFS we consider the strategic storage of file how can happen? Also due to its feature distributed hash Table which satisfy in decentralisation, fault tolerance and scalability. In term block exchange it generates version of bit swap (Rahalkar and Gujar, 2019) in it. It also has a feature like Merkle DAG properties (Becker, 2008). This assures that the exchange of data blocks on peer to peer networks is reliable, undamaged and unchanged. Due to its property it gives high-throughput.

  Consider when u try to upload the file in to the browser or cloud i just consider browser as a single node when its being submitted toward its the cloud hence we store the file through the Interplanetary file system storage. As we know when we store the file or Image using IPFS first is converted to raw bit which can be binary bit that's computer understands. Then raw bit for the image/file is undergo message digestion or hash function like SHA-256 to get unique touches to address them IPFS created a content identifier or CID. This content Identifier is multihash value which its self-describing hash format in hexadecimal. The output gives fixed encoded length of 58 bits which is with hash value of 'Qm...' as shown in Figure 3.

  After the hash value is retrieved from where it is stored in Blockchain where, unless the agreement is accepted, the blocks are created by using the smart contract which is considered as negotiation of the agreement between the peer to peer networks.

- *Blockchain:* This is technology that's implements a stable, decentralised, distributed, autonomous secure database. It has used for creating autonomous computer systems known as 'smart contract', in speeding up transfers, developing financial instruments, organising in exchange of data and information. For the case and issue of distributed network or peer to peer network face the different attack such as Sybil attack (Buterin, 2014; Douceur, 2002; Zhang and Lee, 2020b). Hence the idea of the blockchain technology concept of the distributed consensus algorithm tries to reduce it. Hence, we consider the Ethereum blockchain in our case it has the feature of computation power (i.e., proof of work to be done). Another feature of it is a permission less block chain hence any one can observe it. The reason of using this concept as auditing in blockchain it's that

  1 prevent from tampering of information which is being stored
  2 when store hash value in public blockchain no one will understand or figure out what is being stored to other users in blockchain network since the will be the only user can understand it.

3.2 Data plane

Cloud storage reduces local storage requirements and enables efficient file sharing. Conventional cloud storage is a centralised system that provides all services on the basis of a trusted party. Second, data on cloud storage is open, modifiable and removable by the cloud provider in such a centralised architecture. According to the hash value retrieve back from IPFS it will be stored in cloud also for every action is being stored in cloud for the case of our experiment we will store hash value obtain by IPFS in blockchain and cloud simultaneous. In order whatever we stored them can record both sides.

4 Experiment and result

4.1 Setup

In our experiment, due to the real scenario of blockchain in Ethereum, we consider a simulation and the following technology requirements as shown in Table 1.

Table 1 Technologies used for implementation

Technology	*Version*
Node.js	v13.8.0
Truffle	v5.1.6 (core: 5.1.6)
Web3.js	v1.2.1
Ganache	2.1.2
Ipfs-http-client	41.0.1

From the perspective of design, during collecting the image data or IoT data we have to restore in image in form of Buffer during uploading as shown below for Process file for IPFS as shown below.

Process IoT data/file for IPFS

```
// we fetch file/data from event
1   const file = event.target.files[0]
    // convert file/data into buffer
2   const reader = new window.FileReader()
3   reader.readAsArrayBuffer(file)
4   reader.onloadend = () => {
5   this.setState({ buffer: Buffer(reader.result) }) }
```

The required from the code shown above during processing file and file is forwarded into buffer before processing into IPFS. During this process of collecting data, and to add IoT data in IPFS and retrieve a hash value. Consider IPFS client mode to be used in connecting them using the blow shown algorithm.

Add and return, and hash value from IPFS and stored in Blockchain

```
// collect the buffer data into Ipfs
1    ipfs.add(this.state.buffer, (error, result) => {
// print out to console when the Ipfs has being succeed
2      console.log('Ipfs responding...', result)
// retrieve back the hash value when succeed from Ipfs
3      const mwikaHash = result[0].hash
// set the hash value has object for process for smart contract to be process
4      this.setState({ mwikaHash})
// when error occur during Ipfs collecting the buffer data
5      if (error) {
     print out error occur in console
6        console.error(error);
7        return
8      } // call the set function from smart contract and pass the hash value
9      this.state.contract.methods.set(mwikaHash).send({
10       from: this.state.account }).then((r) => {
11       return this.setState({ mwikaHash })
12   })
```

For the system to achieve we have to connect with our smart contract which generated from Ethereum blockchain. Hence, from the blockchain code scenario we have used a solidity program as shown below.

Smart contract

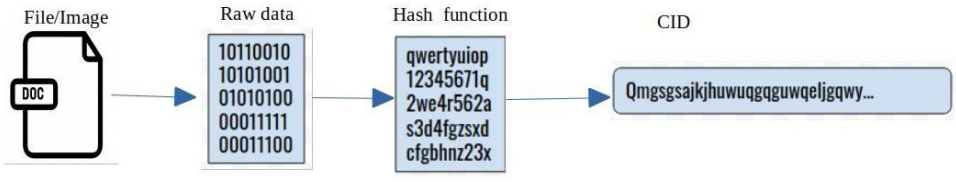
```
// declare smart contract
1   contract Mwika {          // create state variable
2   string mwikaHash;         // function created for writing or set variable
3   function set(string memory _mwikaHash) public {
4   mwikaHash = _mwikaHash;
5   }                         // function created for read or obtain variable
6   function get() public view returns(string memory) {
7   return mwikaHash;
8   } }
```

4.2 Result

From the analysis of IoT data or image data sent to IPFS, Our proposed system is designed in such way that the IPFS is able to send the multi hash value to the cloud data plane for storing and also return the hash value to the blockchain simultaneously for generating the blocks as shown in the Figure 2. From below we can observe the sample of the result we obtain to and similar the amount of Gas used per every transaction we observe less than 0.0025 ether (0.001234 ether) as shown in Figure 3. It can be observed

that the IPFS has recorded the data Image /hash value of every sample after every transaction.

Figure 3 IPFS working model (see online version for colours)



The samples of result have taken during uploading data image respectively and also in below we check some of the transaction have being recorded it as shown in Figure 4.

Figure 4 Data image received and recorded by the proposed blockchain system (see online version for colours)

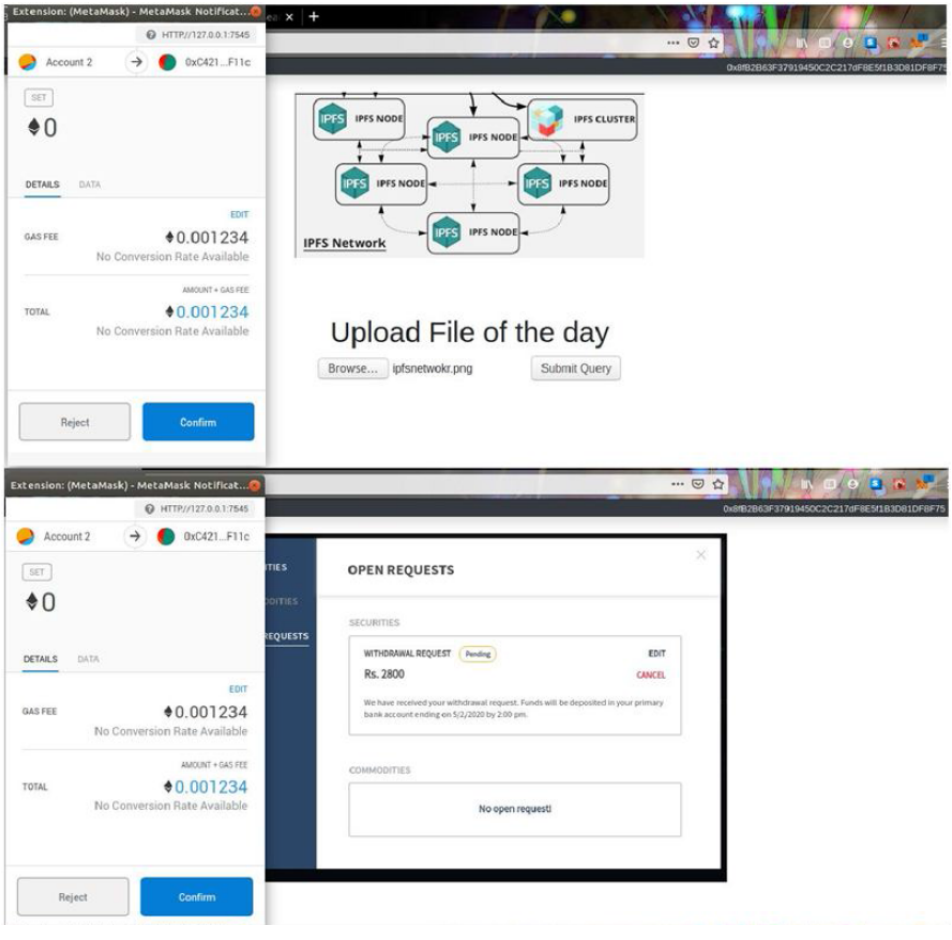


Figure 4 Data image received and recorded by the proposed blockchain system (continued) (see online version for colours)

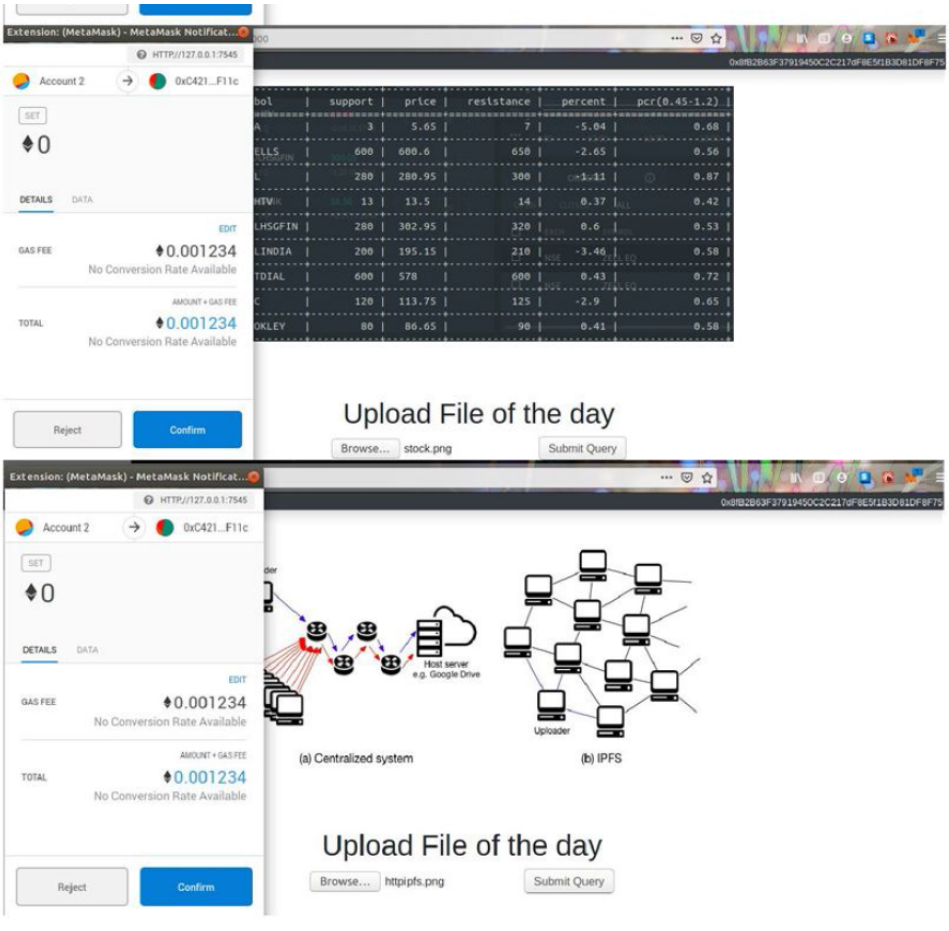
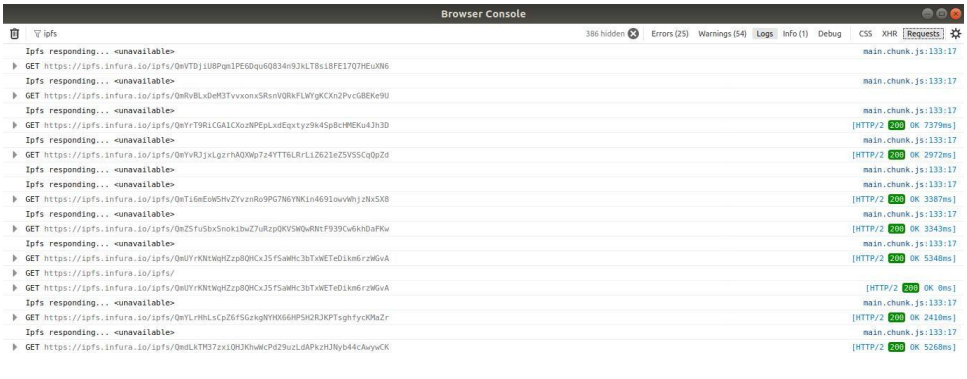
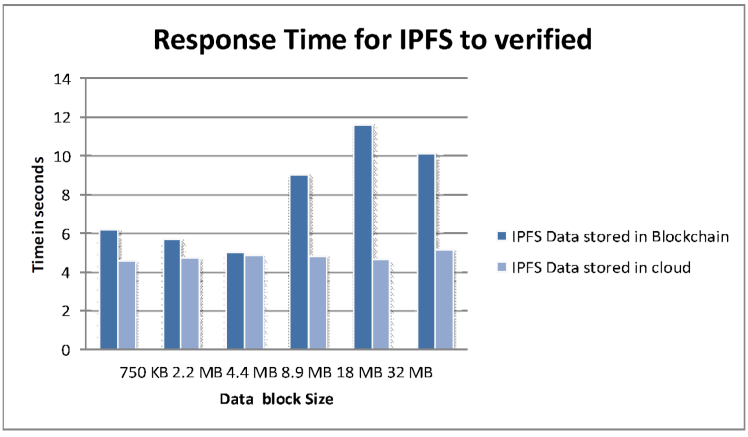


Figure 5 IPFS recorded the data Image /hash value of every sample (see online version for colours)



To perform privacy and security analysis, an adversary would try to observe what is happening by forging the digital signature in order to alter the access permission in the blockchain, but the nature of perspective data which is being stored in a block will still be the multi hash value generated from IPFS. However, the blockchain is public; hence it would be rigid for the adversary to understand it as shown in Figure 5.

Figure 6 Time spent for retrieved IPFS hash value (see online version for colours)



In term of Integrity of IoT data we consider the time response for the hash value to be send in to the cloud successful and to be stored in blockchain as observed from Figure 6. This show hash value of the data present at cloud and from where it was collected is matched.

5 Conclusions

From our perspective, we succeeded in design a secure data storage system that can be audited and regulated, particularly for IoT data, by the nature of our primary design. Moreover, we also succeeded in utilising data plane storage. We are currently finalising a complete reference implementation of our framework and developing a range of IoT applications.

References

Ali, M., Nelson, J., Shea, R. and Freedman, M.J. (2016) 'Blockstack: a global naming and storage system secured by blockchain', *2016 Annual Technical Conference ({USENIX}{ATC})*, pp.181–194.

Asghar, M.R., Ion, M., Russello, G. and Crispo, B. (2012) 'Securing data provenance in the cloud', *Open Problems in Network Security*, pp.145–160, Springer, Berlin, Heidelberg.

Becker, G. (2008) *Merkle Signature Schemes, Merkle Trees and their Cryptanalysis*, Ruhr-University Bochum, Tech. Rep, Bochum, Germany.

Benet, J. and Greco, N. (2018) *Filecoin: A Decentralized Storage Network*, Protocol Labs, Tech. Rep, San Francisco, CA, USA.

Buterin, V. (2014) 'Long-range attacks: the serious problem with adaptive proof of work', *Ethereum Blog*, Ethereum.

Carzaniga, A., Rosenblum, D.S. and Wolf, A.L. (2000) *Content-Based Addressing and Routing: A General Model and its Application*, Technical Report CU-CS-902-00, Department of Computer Science, University of Colorado, USA.

Douceur, J.R. (2002) 'The Sybil attack', *International Workshop on Peer-To-Peer Systems*, Springer, Berlin, Heidelberg, pp.251–260.

Ion, I., Sachdeva, N., Kumaraguru, P. and Čapkun, S. (2011) 'Home is safer than the cloud! Privacy concerns for consumer cloud storage', *Proceedings of the Seventh Symposium on Usable Privacy and Security*, July, pp.1–20.

Lodderstedt, T., McGloin, M. and Hunt, P. (2013) 'OAuth 2.0 threat model and security considerations', *IETF2013*.

Panarello, A., Tapas, N., Merlino, G., Longo, F. and Puliafito, A. (2018) 'Blockchain and IoT integration: a systematic survey', *Sensors*, Vol. 18, No. 8, p.2575.

Rahalkar, C. and Gujar, D. (2019) 'Content addressed P2P file system for the web with blockchain-based meta-data integrity', *2019 6th IEEE International Conference on Advances in Computing, Communication and Control*.

Shafagh, H., Burk halter, L., Hithnawi, A. and Duquennoy, S. (2017) 'Towards blockchain-based auditable storage and sharing of IoT data', *Proceedings of the 2017 on Cloud Computing Security Workshop*, pp.45–50.

Tikhomirov, S., Voskresenskaya, E., Ivanitskiy, I., Takhaviev, R., Marchenko, E. and Alexandrov, Y. (2018) 'Smart check: static analysis of Ethereum smart contracts', *Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain*, pp.9–16.

Wilkinson, S., Bolsheviks, T., Brandoff, J. and Buterin, V. (2014) *Storj a Peer-to-Peer Cloud Storage Network*, Storj Lab. Inc., Atlanta, GA, USA, Tech. Rep.

Wright, C.S. (2019) 'Bitcoin: a peer-to-peer electronic cash system', *SSRN Electronic Journal*, pp.1–9.

Xie, C., Sun, Y. and Lou, H. (2017) 'Secured data storage scheme based on block chain for agricultural products tracking', *2017 3rd International Conference on Big Data Computing and Communications (BIGCOM)*, IEEE, pp.45–50.

Zachariah, T., Klugman, N., Campbell, B., Adkins, J., Jackson, N. and Dutta, P. (2015) 'The internet of things has a gateway problem', *Proceedings of the 16th International Workshop on Mobile Computing Systems and Applications*, pp.27–32.

Zhang, B., Mor, N., Kolb, J., Chan, D.S., Lutz, K., Allman, E., Wawrzynek, J., Lee, E. and Kubiatowicz, J. (2015) 'The cloud is not enough: Saving IoT from the cloud', *7th USENIX Workshop on Hot Topics in Cloud Computing (Hot Cloud 15)*.

Zhang, S. and Lee, J-H. (2020a) 'A group signature and authentication scheme for blockchain-based mobile edge computing', *IEEE Internet of Things Journal*, Vol. 7, No. 5, pp.4557–4565.

Zhang, S. and Lee, J-H. (2020b) 'Mitigations on Sybil-based double spend attacks in bitcoin', *IEEE Consumer Electronics Magazine*, Vol. 9, No. 6, p.1.